Quantum algorithms 2021/2022: Final exam

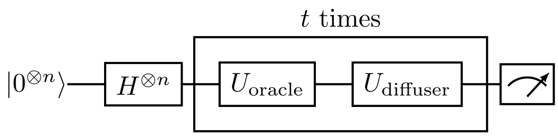
Benoît Vermersch (benoit.vermersch@lpmmc.cnrs.fr) - 2022 Jan 17th, 13:30-15:30 (2 hours)

- The exam consists of two problems.
- Documents allowed: Slides of the lectures, documents of the exercices, hand-written notes
- You can only use your laptop to look at the documents from Moodle.
- You can also use printed versions of these documents.
- The use of smartphones or tablets is not allowed.

1 Grover's algorithm with multiple solutions ($\approx 7/20$)

We define a $n-$bit Boolean function $f(x)$, $x = (x_1, \dots, x_n)$. We assume the existence of $M \geq 1$ distinct solutions $w_{m=1,\dots,M}$, such that $f(w_m) = 1$.

Grover's algorithm is implemented via the following quantum circuit (cf Lecture 2):



with $U_{\text{oracle}} |x\rangle = (-1)^{f(x)} |x\rangle$, and $U_{\text{diffuser}} = 2 |\psi\rangle \langle\psi| - 1$, $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$.

1. Write the state $|\psi_0\rangle$ before the first application of the oracle, as a function of $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \neq w_m} |x\rangle$ and $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{w_m} |w_m\rangle$. You can introduce the angle θ, defined as $\sin(\theta/2) = \sqrt{M/N}$, $\cos(\theta/2) = \sqrt{(N-M)/N}$.

   Solution: c.f Exercices 2 $|\psi_0\rangle = |\psi\rangle$ (equal superposition on each bitstring), which can be rewritten as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle = \cos(\theta/2) |\alpha\rangle + \sin(\theta/2) |\beta\rangle \tag{1}$$

   with $\sin(\theta/2) = \sqrt{M/N}$, $\cos(\theta/2) = \sqrt{(N-M)/N}$.

2. Write how the two states $|\alpha\rangle$, $|\beta\rangle$ are transformed after application of the diffuser. **Solution:** You can use the expression of the diffuser

$$U_{\text{diffuser}} |\alpha\rangle = \cos(\theta) |\alpha\rangle + \sin(\theta) |\beta\rangle \tag{2}$$
$$U_{\text{diffuser}} |\beta\rangle = -\cos(\theta) |\beta\rangle + \sin(\theta) |\alpha\rangle \tag{3}$$

3. Write the state $|\psi_{t=1}\rangle$ after the first iteration of the circuit.

   Solution: The oracle first changes the sign of the β amplitude, thus we obtain

$$|\psi_1\rangle = U_{\text{diffuser}} (\cos(\theta/2) |\alpha\rangle - \sin(\theta/2) |\beta\rangle) = \cos(3\theta/2) |\alpha\rangle + \sin(3\theta/2) |\beta\rangle \tag{4}$$

4. Write the state $|\psi_t\rangle$ after an arbitrary number of iterations.

   Solution: Following the same derivation we find

$$|\psi_t\rangle = \cos((2k+1)\theta/2) |\alpha\rangle + \sin((2k+1)\theta/2) |\beta\rangle \tag{5}$$

5. Express the probability p to measure a bitstring x that belongs to the set of solutions, i.e such that $x \in \{w_1, \dots, w_M\}$, after t iterations. Why is it important here to know in advance the value of M? Simplify the expression in the limit of small $\theta \ll 1$ and large number of iterations $t \gg 1$.

   Solution: The probability to observe an arbitray solution is

$$p = \sum_m | \langle w_m | \psi_t \rangle |^2 = \sin((2t+1)\theta/2)^2 \sum_m | \langle w_m | \beta \rangle |^2 = \sin((2t+1)\theta/2)^2 \tag{6}$$

   In the limit of small θ (large N) and large t, we obtain $\theta/2 \approx \sin(\theta/2) = \sqrt{M/N}$. Thus

$$p \approx \sin(2t\sqrt{M/N})^2 \tag{7}$$

6. Express the condition on the number of iterations t to observe a solution with high probability p. Express how such required value of t scales with N and M. Compare with the case $M = 1$ shown in Lecture 2.

   Solution: $p \approx 1$ for $2t\sqrt{M/N} \approx \pi/2$, i.e for $t \approx (\pi/4)\sqrt{N/M}$. Obviously, the required t decreases with increasing number of solutions M.

2 Quantum error correction with the five qubit code ($\approx 13/20$)

The five qubit code is a quantum error correction code that uses five physical qubits to encode one logical qubit.

2.1 Defining the code

1. Explain the meaning of a physical, and of a logical qubit.

   Solution: c.f. lecture 3

2. The five qubit code can be described in terms of a $[5, 1]$ stabilizer code, with the stabilizer group S generated by 4 elements

$$\begin{aligned} g_1 &= X_1Z_2Z_3X_4 \\ g_2 &= X_2Z_3Z_4X_5 \\ g_3 &= X_1X_3Z_4Z_5 \\ g_4 &= Z_1X_2X_4Z_5. \end{aligned}$$

   Show that such group S fulfills the conditions for being a stabilizer group.

   Solution: c.f. lecture 3, all generators are members of the Pauli group, and commute. This means that the generated group S is an abelian group of the Pauli group. Moreover, the group does not contain $-I$. The group S therefore corresponds to the definition of a stabilizer group.

3. Explain how one can *formally* define the code world $\{|0\rangle_L, |1\rangle_L\}$, i.e the Hilbert space of dimension 2 defining the logical qubit, based on the stabilizer group.

   Solution: C.f. Lecture 3, The stabilizer group has a minimal representation with 4 generators, and 5 physical qubits. Therefore, the vector space stabilized by the stabilizer group is of dimension 2^k with $k = 5 - 4 = 1$. This means we can encode one logical qubit. Formally, the vector space denotes all vectors $|\psi\rangle$ such $g_i |\psi\rangle = |\psi\rangle$. The states $|0\rangle_L$, and $|1\rangle_L$ denote one choice of orthonornal basis for this vector space.

4. Calculate analytically the error syndromes for an error X_1 on the first qubit.

   Solution:

$$\langle g_1 \rangle = \langle \psi | X_1(X_1Z_2Z_3X_4)X_1 |\psi\rangle = \langle \psi | g_1 |\psi\rangle = 1 \tag{8}$$

   as the logical qubit state $|\psi\rangle$ is stabilized by g_1. Similarly, we obtain $\langle g_2 \rangle = 1$, $\langle g_3 \rangle = 1$. Finally

$$\langle g_4 \rangle = \langle \psi | X_1(Z_1X_2X_4Z_5)X_1 |\psi\rangle = -\langle \psi | g_4 |\psi\rangle = -1. \tag{9}$$

5. Without further calculations, list in a table the possible error syndromes for each qubit error. Show that each single qubit error can be detected and corrected.

   Solution:

Error	Syndrome g_1, g_2, g_3, g_4	Error	Syndrome g_1, g_2, g_3, g_4	Error	Syndrome g_1, g_2, g_3, g_4
I	1,1,1,1				
X_1	1,1,1,-1	Z_1	-1,1,-1,1	Y_1	-1,1,-1,-1
X_2	-1,1,1,1	Z_2	1,-1,1,-1	Y_2	-1,-1,1,-1
X_3	-1,-1,1,1	Z_3	1,1,-1,1	Y_3	-1,-1,-1,1
X_4	1,-1,-1,1	Z_4	-1,1,1,-1	Y_4	-1,-1,-1,-1
X_5	1,1,-1,-1	Z_5	1,-1,1,1	Y_5	1,-1,-1,-1

   The recovery operation is simply the error operator (Example a X_1 error is corrected via a X_1 operation, as $X_1^2 = I$).

6. Show that the following states can be used to define a logical qubit

$$\begin{aligned} |0\rangle_L &= \prod_i (1 + g_i) |0\rangle^{\otimes N} \\ |1\rangle_L &= \prod_i (1 + g_i) |1\rangle^{\otimes N} \end{aligned} \tag{10}$$

Solution:

$$g_k \left|0\right\rangle_L = g_k \prod_i (1+g_i) \left|0\right\rangle^{\otimes N} = \prod_{i\neq k} (1+g_i)(g_k+g_k^2) \left|0\right\rangle^{\otimes N} = \left|0\right\rangle_L \tag{11}$$

because $g_k^2 = 1$. Same thing for the orthogonal logical 1 state

7. Show that $Z_L = Z_1Z_2Z_3Z_4Z_5$ and $X_L = X_1X_2X_3X_4X_5$ can be used as single qubit logical gates. Write also the expression of the logical Y_L gate as a function of the physical qubits operators.

   Solution:

$$\begin{aligned}
X_L \left|0_L\right\rangle &= \prod_i (1+g_i)\, X_L \left|0\right\rangle^{\otimes N} = \left|1_L\right\rangle \\
X_L \left|1_L\right\rangle &= \prod_i (1+g_i)\, X_L \left|1\right\rangle^{\otimes N} = \left|1_L\right\rangle \\
Z_L \left|0_L\right\rangle &= \prod_i (1+g_i)\, Z_L \left|0\right\rangle^{\otimes N} = \left|1_L\right\rangle \\
Z_L \left|1_L\right\rangle &= \prod_i (1+g_i)\, Z_L \left|1\right\rangle^{\otimes N} = -\left|1_L\right\rangle
\end{aligned} \tag{12}$$

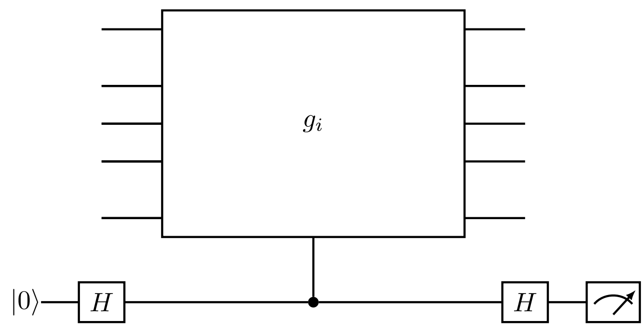
   as each g_i commutes with X_L. X_L and Z_L perform the required operation on the logical qubits, they can be thus defined as our logical qubit operators. Up to an irrelevant global phase, we can define $Y_L = X_L Z_L$.

2.2 Stabilizer measurement

1. Explain why we need an ancilla qubit to perform an error syndrome.

   Solution: c.f. Exercices 3: We need a projective measurement on a collective operator g_i. This can only be achieved via an ancilla qubit.

2. We consider the following measurement circuit. We denote with $\left|\psi\right\rangle$ the wavefunction of the five physical qubits prior to the coupling to the ancilla qubit. Write the two probabilities $p(0)$, $p(1)$ to meaure the ancilla qubit in the state 0, and 1, respectively.



   Solution: The state is transformed as

$$\left|\psi\right\rangle\left|0\right\rangle \to \left|\psi\right\rangle(\left|0\right\rangle+\left|1\right\rangle) \to (\left|\psi\right\rangle\left|0\right\rangle + g_i\left|\psi\right\rangle\left|1\right\rangle) \to (\left|\psi\right\rangle(\left|0\right\rangle+\left|1\right\rangle) + g_i\left|\psi\right\rangle(\left|0\right\rangle-\left|1\right\rangle)) \tag{13}$$

   Therefore the measurement probabilities for the ancilla read

$$\begin{aligned}
p(0) &= |\left\langle\psi\right|(1+g_i)\left|\psi\right\rangle|^2/2 \\
p(1) &= |\left\langle\psi\right|(1-g_i)\left|\psi\right\rangle|^2/2
\end{aligned} \tag{14}$$

3. Show that we can write any g_i in terms of two projector operators $P_i(\pm 1)$, such that $g_i = P_i(1) - P_i(-1)$ with $P_i(1) + P_i(-1) = 1$.

   Solution: As an Hermitian operator, g_i can be decomposed in terms of real eigenvalues ϵ and corresponding projecting operators on the different eigenstates.

$$g_i = \sum_\epsilon \epsilon \left(\sum_{\left|\nu\right\rangle, g_i\left|\nu\right\rangle = \epsilon\left|\nu\right\rangle} \left|\nu\right\rangle\left\langle\nu\right| \right) = \sum_\epsilon \epsilon P_i(\epsilon), \tag{15}$$

   with $\sum_\epsilon P_i(\epsilon) = 1$.

   We use $g_i^2 = 1$. Therefore, g_i has two eigenvalue $\epsilon \pm 1$ (as for any Pauli operator).

4. Show that the ancilla measures the probabilities that the state $|\psi\rangle$ belongs to the eigenvalue ± 1 of the operator g_i, i.e that

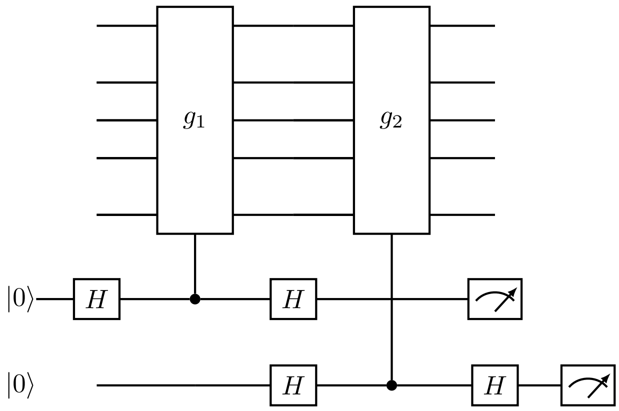
$$\begin{aligned} p(0) &= |\langle\psi|\, P_i(1)\, |\psi\rangle\,|^2 \\ p(1) &= |\langle\psi|\, P_i(-1)\, |\psi\rangle\,|^2. \end{aligned} \tag{16}$$

Interpret this result: Does this circuit correctly perform an error syndrome?

Solution: We use $1 \pm g_i = P_i(1) + P_i(-1) \pm (P_i(1) - P_i(-1)) = 2P_i(\pm 1)$ and obtain that $p(0)$ measures the probability that the state is in the $\epsilon = 1$ subspace. This means that, if we measure the ancilla in the 0 state, we project the state on the $\epsilon = 1$ subspace, where the error syndrome g_i reveals no errors. Conversely, If we detect 1, we detect an error and project via $P_i(-1)$ the state $|\psi\rangle$ onto the corresponding "error" subspace.

5. Briefly explain how to write a full circuit for performing error detection and correction (I am not asking to write down the full circuit explicitely).

Solution: We just need to concatenate the circuits for each stabilizer measurement, using a new ancilla for each g_i. For illustration, the circuit for measuring the first two stabilizers read

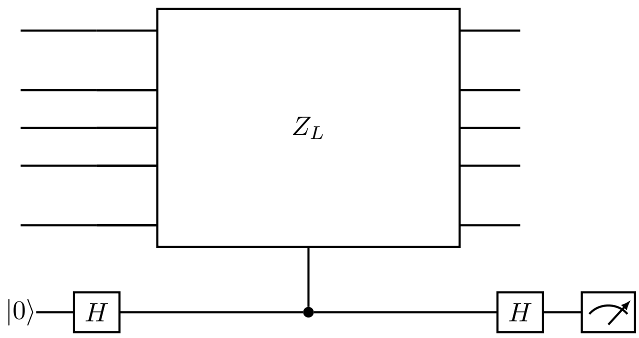


2.3 Encoding a quantum state

1. Explain a strategy to initialize a logical qubit $|0\rangle_L$ from the initial state $|0\rangle^{\otimes N}$ based on only performing error detection and correction.

Solution: We begin in the state $|0\rangle^{\otimes N}$, and realize the measurement of g_1. This projects the state on $P_1(\epsilon_1)\,|0\rangle^{\otimes N}$ depending on the measurement of the ancilla. We repeat this operation for g_2, g_3, g_4, leading to an error syndrome $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ that can be decoded using the table given above, and corrected. This leads to a random superposition $|\psi\rangle_L = a\,|0\rangle_L + b\,|1\rangle_L$, with a, and b *unknown.*

To create the state $|0\rangle_L$, we realize an ancilla assisted measurement of Z_L



If we measure $|0\rangle$, we have successfully prepare the $+1$ eigenstates of Z_L , i.e the state $|0\rangle_L$.

2.4 Performance (Bonus questions)

We consider a probability p_e of error on each physical qubit, occuring independently.

1. For the 5 qubit code, express the probability that a logical qubit $|0\rangle_L$ undergoes an error which *cannot* be corrected.

Solution: The code protects against one single qubit errors. Therefore the probability that the state ends up in a state that we cannot correct is

$$p_e(L) = 1 - (1-p)^5 - 5p(1-p)^4 \tag{17}$$

Note that we have neglected the small probability that two identical errors occur (situation which does not harm the logical state).

2. Write the condition on p_e to achieve 'useful' quantum error correction, i.e to obtain that the 5 qubit code performs better than a single physical qubit. Do we satisfy this condition in the limit of small values of $p_e \to 0$?

   Solution: If $p_e(L) < p_e$, the logical error probability is smaller than the error probability for a single qubit. Therefore we require

   $$1 - (1 - p_e)^5 - 5p_e(1 - p_e)^4 < p_e \tag{18}$$

   For $p_e \to 0$, $p_e(L) \approx 1 - 1 + 5p_e - 5p_e + O(p^2) \ll p_e$. This makes sense: when $p_e \to 0$, the probability of having two errors becomes negligible compared to the probability of having a single error, and quantum error correction becomes useful.